5

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－171717

(43)公開日　平成10年(1998)６月26日

(51)Int.Cl.⁶	識別記号	ＦＩ	
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｅ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ａ
9/10			６０１Ｂ
			６０１Ｅ

審査請求　未請求　請求項の数３　ＯＬ　（全８頁）　最終頁に続く

(21)出願番号　特願平8－324942

(22)出願日　平成８年(1996)12月５日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　高木　伸哉
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　梅原　紀夫
大阪府門真市大字門真1006番地　松下電器産業株式会社内

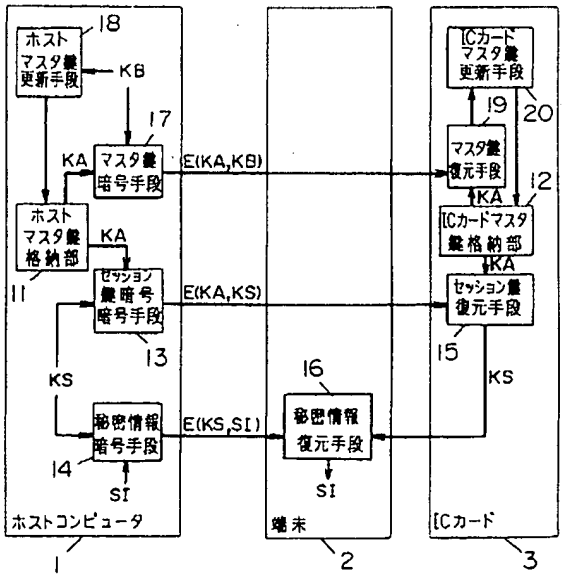
(74)代理人　弁理士　滝本　智之　（外１名）

(54)【発明の名称】　ＩＣカードおよびそれを用いた暗号通信システム

(57)【要約】

【課題】　ホストコンピュータと端末間で通信される暗号化データを盗聴され、かつ暗号鍵を管理するＩＣカードが盗まれても安全な暗号通信システムを提供する。

【解決手段】　ホストコンピュータ１は現在のマスタ鍵Ｍによって新しいマスタ鍵Ｎを暗号化しＩＣカード３に送る。ホストコンピュータ１とＩＣカード３は、マスタ鍵によりセッション鍵を暗号化して配送する毎に，自身のマスタ鍵Ｍを新しいマスタ鍵Ｎに更新する。これにより，セッション鍵およびそれによって暗号化された秘密情報の解読を防ぐことができる。



1

【特許請求の範囲】

【請求項１】　暗号通信に用いるマスタ鍵Ｎもしくはセッション鍵を暗号化、復号化するためのマスタ鍵Ｍを格納するＩＣカードマスタ鍵格納部と、外部から受信した暗号化されたマスタ鍵Ｎデータを復号化して、マスタ鍵Ｎを復元するマスタ鍵復元手段と、現在のマスタ鍵Ｍもしくはマスタ鍵Ｎを用いて外部から受信した暗号化されたセッション鍵データを復号化して、暗号通信を行う度にランダムに生成されるセッション鍵を復元するセッション鍵復元手段と、前記マスタ鍵復元手段からの出力を受け、前記ＩＣカードマスタ鍵格納部に格納されている現在のマスタ鍵Ｍをマスタ鍵Ｎに更新するＩＣカードマスタ鍵更新手段とを備えたことを特徴とするＩＣカード。

【請求項２】　ＩＣカードマスタ鍵格納部に格納されているマスタ鍵Ｍを用いて、外部から受信した暗号化されたセッション鍵データを復号化し、セッション鍵を復元し、外部へ送信するセッション鍵復元手段と、セッション鍵の復元後に前記ＩＣカードマスタ鍵格納部に格納されているマスタ鍵Ｍを用いて、外部から受信した暗号化されたマスタ鍵Ｎデータを復号化するマスタ鍵復元手段と、前記マスタ鍵復元手段からの出力を受け、前記ＩＣカードマスタ鍵格納部に格納されている現在のマスタ鍵Ｍをマスタ鍵Ｎに更新するＩＣカードマスタ鍵更新手段とを備えたことを特徴とする請求項１記載のＩＣカード。

【請求項３】　ホストコンピュータと、前記ホストコンピュータに接続される端末と、前記端末に着脱可能な状態で接続されるＩＣカードとを有し、

前記ホストコンピュータは、マスタ鍵Ｎもしくはセッション鍵を暗号化、復号化するためのマスタ鍵Ｍを格納するホストマスタ鍵格納部と、前記ホストコンピュータにおいて新たに生成したマスタ鍵Ｎを暗号化して、マスタ鍵Ｎデータを送信するマスタ鍵暗号手段と、暗号通信を行う度にランダムに生成されるセッション鍵を暗号化してセッション鍵データを送信するセッション鍵暗号手段と、秘密情報を暗号化して秘密情報データを送信する秘密情報暗号手段と、前記ホストマスタ鍵格納部に格納されている現在のマスタ鍵Ｍをマスタ鍵Ｎに更新するホストマスタ鍵更新手段とを備え、

前記ＩＣカードは、マスタ鍵Ｍを格納するＩＣカードマスタ鍵格納部と、外部から受信したセッション鍵データを復号化して、セッション鍵を復元し、前記端末にセッション鍵を送信するセッション鍵復元手段と、外部から受信したマスタ鍵Ｎデータを復号化して、マスタ鍵Ｎを復元するマスタ鍵復元手段と、前記マスタ鍵復元手段からの出力を受け、前記ＩＣカードマスタ鍵格納部に格納されている現在のマスタ鍵Ｍをマスタ鍵Ｎに更新するＩＣカードマスタ鍵更新手段とを備え、

前記端末は、前記ＩＣカードから受信したセッション鍵

2

を用いて、前記ホストコンピュータから受信した秘密情報データを復号化して、秘密情報を復元する秘密情報復元手段を備えた暗号通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はマイクロプロセッサとメモリを内蔵し、ＩＣカード使用者の正当性確認、マスタ鍵Ｍの保管用等に使用されるＩＣカードおよびそれを用いた暗号通信システムに関する。

【０００２】

【従来の技術】ホストコンピュータと端末間で暗号通信を行う際、安全性を高めるため暗号通信に用いる鍵を毎回変えることが望ましい。このために、鍵を暗号化するためのマスタ鍵Ｍを双方で共有し、これを用いて、実際の暗号通信に使用されるマスタ鍵Ｎもしくはセッション鍵を暗号化して秘密暗号鍵として安全に配送する。この実際の暗号通信に使用される鍵であるセッション鍵は、その場限りに使用される鍵として、暗号通信を行う度にランダムに生成される。

【０００３】従来の暗号通信システムについて、図３を用いて説明する。図３では、ホストコンピュータ１０１と端末１０２間で秘密暗号鍵を用いて暗号通信を行う場合を示している。ホストコンピュータ１０１はホストマスタ鍵格納部１１１にマスタ鍵Ｍ・ＫＭを有している。もう一方のマスタ鍵Ｍ・ＫＭを端末１０２内に格納すると、不正者により端末１０２に格納されているマスタ鍵Ｍ・ＫＭが盗まれる可能性があるため、物理的に安全な、すなわち内部のデータを不正に外から読み書きすることができないＩＣカード１０３のＩＣカードマスタ鍵格納部１１２内に格納されている。

【０００４】以下に暗号通信の流れを示す。まずホストコンピュータ１０１はセッション鍵ＫＳをランダムに生成する。第１の暗号手段１１３は、ホストマスタ鍵格納部１１１に格納されているマスタ鍵Ｍ・ＫＭによりセッション鍵ＫＳを暗号化したセッション鍵データＥ（ＫＭ，ＫＳ）を、端末１０２を介してＩＣカード１０３に送る。ＩＣカード１０３の第１の復元手段１１４は受信したセッション鍵データＥ（ＫＭ，ＫＳ）を、ＩＣカードマスタ鍵格納部１１２に格納されているマスタ鍵Ｍ・ＫＭにより復号化してセッション鍵ＫＳを復元し、これを端末１０２へ送る。

【０００５】これにより、ホストコンピュータ１０１と端末１０２は同じセッション鍵ＫＳを共有したこととなり、このセッション鍵ＫＳを用いて秘密情報ＳＩの暗号通信を行う。具体的には、ホストコンピュータ１０１の第２の暗号手段１１５がセッション鍵ＫＳにより本来通信すべき情報である秘密情報ＳＩを暗号化した秘密情報データＥ（ＫＳ，ＳＩ）を生成して端末１０２に送り、端末１０２の第２の復元手段１１６がこの秘密情報データＥ（ＫＳ，ＳＩ）をＩＣカード１０３より送られてき

3

たセッション鍵ＫＳにより復号化し、秘密情報ＳＩを復元する。

【０００６】ここで、第２の復元手段１１６による処理は端末１０２内で行うよりも、物理的に安全なＩＣカード１０３内で行う方がセキュリティは高くなるが、ＩＣカード１０３は処理能力に限界があるため、秘密情報ＳＩが長い電文である場合等は復号化に時間がかかる。そのため、暗号化された秘密情報ＳＩの復号処理は端末１０２内で行い、ＩＣカード１０３は鍵の管理、すなわちマスタ鍵Ｍ・ＫＭの保管およびセッション鍵ＫＳの復元のみを行っている。

【０００７】従って、例えば端末１０２とＩＣカード１０３が通信を行う時は、ＩＣカード１０３が端末１０２内に取り込まれる等、端末１０２とＩＣカード１０３間の通信は安全であることが必要である。しかしながら実際には、端末１０２とＩＣカード１０３がケーブル等で接続される場合であっても、その間の通信を盗聴できる者は限定されるため、比較的安全である。

【０００８】

【発明が解決しようとする課題】ところが、ホストコンピュータと端末間の通信には公衆回線を使用する場合が多く、この間を伝送されるデータ、すなわちセッション鍵データＥ（ＫＭ，ＫＳ）および秘密情報データＥ（ＫＳ，ＳＩ）は容易に盗聴され得る。これらはいずれも暗号化されているため、それだけで秘密情報が洩れる心配はないが、盗聴した不正者が更にＩＣカードを盗んだ場合、盗聴したセッション鍵データＥ（ＫＭ，ＫＳ）を盗んだＩＣカードに入力すれば、第１の復元手段がこれを復号化してセッション鍵を外部に出力するため、不正者はセッション鍵を知ることができる。従って、不正者はセッション鍵と盗聴した秘密情報データＥ（ＫＳ，ＳＩ）とから秘密情報を知ることができるという問題点があった。

【０００９】通常、ＩＣカードは盗まれても使用できないよう使用者自身の設定した暗証番号でロックをかけているが、暗証番号は誕生日など簡単な数値の組み合わせにしている使用者も多く、第３者に知られやすいものであり、安全であるとは言い難い。

【００１０】本発明はこのような問題点を解決するために、ホストコンピュータと端末間で通信される暗号化データを盗聴され、かつ鍵を管理するＩＣカードが盗まれても安全なＩＣカードおよびそれを用いた暗号通信システムを提供することを目的とする。

【００１１】

【課題を解決するための手段】上記目的を達成するために本発明のＩＣカードは、暗号通信に用いるマスタ鍵Ｎもしくはセッション鍵を暗号化、復号化するためのマスタ鍵Ｍを格納するＩＣカードマスタ鍵格納部と、外部から受信した暗号化されたマスタ鍵Ｎデータを復号化して、マスタ鍵Ｎを復元するマスタ鍵復元手段と、現在のマスタ鍵Ｍもしくはマスタ鍵Ｎを用いて外部から受信した暗号化されたセッション鍵データを復号化して、暗号通信を行う度にランダムに生成されるセッション鍵を復元するセッション鍵復元手段と、前記マスタ鍵復元手段からの出力を受け、前記ＩＣカードマスタ鍵格納部に格納されている現在のマスタ鍵Ｍをマスタ鍵Ｎに更新するＩＣカードマスタ鍵更新手段とを備えたものである。

4

【００１２】また本発明の暗号通信システムは、ホストコンピュータと、前記ホストコンピュータに接続される端末と、前記端末に着脱可能な状態で接続されるＩＣカードとを有し、前記ホストコンピュータは、マスタ鍵Ｎもしくはセッション鍵を暗号化、復号化するためのマスタ鍵Ｍを格納するホストマスタ鍵格納部と、前記ホストコンピュータにおいて新たに生成したマスタ鍵Ｎを暗号化して、マスタ鍵Ｎデータを送信するマスタ鍵暗号手段と、暗号通信を行う度にランダムに生成されるセッション鍵を暗号化してセッション鍵データを送信するセッション鍵暗号手段と、秘密情報を暗号化して秘密情報データを送信する秘密情報暗号手段と、前記ホストマスタ鍵格納部に格納されている現在のマスタ鍵Ｍをマスタ鍵Ｎに更新するホストマスタ鍵更新手段とを備え、前記ＩＣカードは、マスタ鍵Ｍを格納するＩＣカードマスタ鍵格納部と、外部から受信したセッション鍵データを復号化して、セッション鍵を復元し、前記端末にセッション鍵を送信するセッション鍵復元手段と、外部から受信したマスタ鍵Ｎデータを復号化して、マスタ鍵Ｎを復元するマスタ鍵復元手段と、前記マスタ鍵復元手段からの出力を受け、前記ＩＣカードマスタ鍵格納部に格納されている現在のマスタ鍵Ｍをマスタ鍵Ｎに更新するＩＣカードマスタ鍵更新手段とを備え、前記端末は、前記ＩＣカードから受信したセッション鍵を用いて、前記ホストコンピュータから受信した秘密情報データを復号化して、秘密情報を復元する秘密情報復元手段を備えたものである。

【００１３】この構成により、セッション鍵を配送する毎にマスタ鍵Ｍを更新することとなり、盗んだＩＣカードに不正者が盗聴した暗号化データを入力しても、もはやそのＩＣカードのマスタ鍵Ｍはマスタ鍵Ｎに更新されており、セッション鍵を得ることはできない。従って、このセッション鍵を用いての暗号化された秘密情報の解読を防止できることとなる。

【００１４】

【発明の実施の形態】以下、本発明の好ましい実施の形態について図面を参照しつつ詳細に説明する。

【００１５】（実施の形態１）図１は本実施の形態における暗号通信システムの構成図であり、ホストコンピュータ１と端末２間で秘密暗号鍵を用いて暗号通信を行う場合を示している。

【００１６】同図において、ホストコンピュータ１はホストマスタ鍵格納部１１に現在のマスタ鍵Ｍ・ＫＡを有

5

している。もう一方の復号化のためのマスタ鍵Ｍ・ＫＡは、端末２内に格納すると端末２からマスタ鍵Ｍ・ＫＡが盗まれる可能性があるため、物理的に安全なＩＣカード３のＩＣカードマスタ鍵格納部１２内に格納されている。

【００１７】暗号通信の手順を順を追って説明する。まずホストコンピュータ１は、セッション鍵ＫＳをランダムに生成する。セッション鍵暗号手段１３で、ホストマスタ鍵格納部１１に格納されているマスタ鍵Ｍ・ＫＡを用いてセッション鍵ＫＳを暗号化したセッション鍵データＥ（ＫＡ，ＫＳ）を、端末２を介してＩＣカード３に送信する。また秘密情報暗号手段１４においては、セッション鍵ＫＳを用いて本来通信すべき情報である秘密情報ＳＩを暗号化した秘密情報データＥ（ＫＳ，ＳＩ）を端末２に送信する。

【００１８】一方、ＩＣカード３側では、セッション鍵復元手段１５が受信したセッション鍵データＥ（ＫＡ，ＫＳ）をＩＣカードマスタ鍵格納部１２に格納されている現在のマスタ鍵Ｍ・ＫＡにより復号化して、セッション鍵ＫＳを復元する。復元されたセッション鍵ＫＳは、端末２に送信する。

【００１９】これにより、ホストコンピュータ１と端末２は同じセッション鍵ＫＳを共有したこととなり、秘密情報復元手段１６が受信した秘密情報データＥ（ＫＳ，ＳＩ）をＩＣカード３から送信されてきたセッション鍵ＫＳにより復号化して、秘密情報ＳＩを復元する。そして復元された秘密情報ＳＩにより様々な処理を行うものである。

【００２０】またホストコンピュータ１はＩＣカード３がセッション鍵を復元した後に、マスタ鍵Ｎ・ＫＢを生成する。マスタ鍵暗号手段１７は、ホストマスタ鍵格納部１１に格納されている現在のマスタ鍵Ｍ・ＫＡによってマスタ鍵Ｎ・ＫＢを暗号化したマスタ鍵ＮデータＥ（ＫＡ，ＫＢ）を、端末２を介してＩＣカード３に送信する。その後、ホストマスタ鍵更新手段１８によって、ホストマスタ鍵格納部１１に格納されている現在のマスタ鍵Ｍ・ＫＡをマスタ鍵Ｎ・ＫＢに更新することで、次回の暗号通信の際はこのマスタ鍵Ｎ・ＫＢがマスタ鍵Ｍ・ＫＡとなる。

【００２１】一方、ＩＣカード３側では、マスタ鍵復元手段１９が受信したマスタ鍵ＮデータＥ（ＫＡ，ＫＢ）をＩＣカードマスタ鍵格納部１２に格納されているマスタ鍵Ｍ・ＫＡにより復号化して、マスタ鍵Ｎ・ＫＢを復元する。その後、ＩＣカードマスタ鍵更新手段２０によって、ＩＣカードマスタ鍵格納部１２に格納されている現在のマスタ鍵Ｍ・ＫＡをマスタ鍵Ｎ・ＫＢに更新することで、次回の暗号通信の際はこのマスタ鍵Ｎ・ＫＢがマスタ鍵Ｍ・ＫＡとなる。

【００２２】ここで、このシステムの安全性について説明する。従来例の場合と同様に、端末２とＩＣカード３

6

間は安全であるが、ホストコンピュータ１と端末２間は非安全であることを前提としている。ホストコンピュータ１と端末２間で伝送されるマスタ鍵ＮデータＥ（ＫＡ，ＫＢ）、セッション鍵データＥ（ＫＡ，ＫＳ）、秘密情報データＥ（ＫＳ，ＫＩ）を不正者が全て盗聴し、さらにＩＣカード３を盗んだとする。この不正者がＩＣカード３の暗証番号を知った場合、盗聴したデータをＩＣカード３に入力し、何らかの出力をＩＣカード３から得ることができるが、ＩＣカード３に格納されているマスタ鍵はもはや以前のマスタ鍵Ｍ・ＫＡではなく、マスタ鍵Ｎ・ＫＢに更新されているため、不正者が欲するセッション鍵ＫＳあるいは秘密情報ＳＩを得ることはできない。

【００２３】すなわち、盗聴したマスタ鍵ＮデータＥ（ＫＡ，ＫＢ）をマスタ鍵復元手段１４に入力しても、ＩＣカードマスタ鍵格納部１２に格納されている鍵は、既にマスタ鍵Ｍ・ＫＡではなくマスタ鍵Ｎ・ＫＢであるため、何ら意味のあるデータを復元することはできない。

【００２４】同様に、盗聴したセッション鍵データＥ（ＫＡ，ＫＳ）をセッション鍵復元手段に入力しても、ＩＣカードマスタ鍵格納部１２に格納されている鍵は、既にマスタ鍵Ｍ・ＫＡではなくマスタ鍵Ｎ・ＫＢであるため、何ら意味のあるデータを復元することはできない。

【００２５】なお、セッション鍵ＫＳを復元した時点と、そのために使用したマスタ鍵Ｍ・ＫＡからマスタ鍵Ｎ・ＫＢへと更新するまでの時点との間が短時間であればあるほど、不正者がセッション鍵データＥ（ＫＡ，ＫＳ）を盗聴してＩＣカード３に入力して情報を得る可能性が減少し、安全性は高くなるので好ましいことは言うまでもない。

【００２６】（実施の形態２）図２は本実施の形態における暗号通信システムの構成図であり、ホストコンピュータ３１と端末３２間で秘密暗号鍵を用いて暗号通信を行う場合を示している。

【００２７】同図において、ホストコンピュータ３１はホストマスタ鍵格納部４１に現在のマスタ鍵Ｍ・ＫＡを有している。もう一方の復号化のためのマスタ鍵Ｍ・ＫＡを端末３２内に格納すると、端末３２からマスタ鍵Ｍ・ＫＡが盗まれる可能性があるため、物理的に安全なＩＣカード３３のＩＣカードマスタ鍵格納部４２内に格納されている。

【００２８】暗号通信の手順を順を追って説明する。まずホストコンピュータ３１はマスタ鍵Ｎ・ＫＢを生成する。マスタ鍵暗号手段４３は、ホストマスタ鍵格納部４１に格納されている現在のマスタ鍵Ｍ・ＫＡによってマスタ鍵Ｎ・ＫＢを暗号化したマスタ鍵ＮデータＥ（ＫＡ，ＫＢ）を、端末３２を介してＩＣカード３３に送信する。その後、ホストマスタ鍵更新手段４４により、ホ

ストマスタ鍵格納部４１に格納されている現在のマスタ鍵Ｍ・ＫＡをマスタ鍵Ｎ・ＫＢに更新し、次回の暗号通信の際はこのマスタ鍵Ｎ・ＫＢがマスタ鍵Ｍ・ＫＡとなる。

【００２９】一方、ＩＣカード３３側では、マスタ鍵復元手段４５が受信したマスタ鍵ＮデータＥ（ＫＡ，ＫＢ）を、ＩＣカードマスタ鍵格納部４２に格納されている現在のマスタ鍵Ｍ・ＫＡにより復号化してマスタ鍵Ｎ・ＫＢを復元する。その後、ＩＣカードマスタ鍵更新手段４６により、ＩＣカードマスタ鍵格納部４２に格納されている現在のマスタ鍵Ｍ・ＫＡをマスタ鍵Ｎ・ＫＢに更新する。ここで述べたホストコンピュータ３１およびＩＣカード３３のマスタ鍵Ｍの配送および更新は、以下に記述するセッション鍵の配送毎に行うものとする。

【００３０】ホストコンピュータ３１はセッション鍵ＫＳをランダムに生成する。セッション鍵暗号手段４７は、ホストマスタ鍵格納部４１に格納されているマスタ鍵Ｎ・ＫＢによりセッション鍵ＫＳを暗号化したセッション鍵データＥ（ＫＢ，ＫＳ）を、端末３２を介してＩＣカード３３に送る。ＩＣカード３３のセッション鍵復元手段４８はこの受信したセッション鍵データＥ（ＫＢ，ＫＳ）を、ＩＣカードマスタ鍵格納部４２に格納されているマスタ鍵Ｎ・ＫＢにより復号化してセッション鍵ＫＳを復元し、これを端末３２へ送る。

【００３１】これにより、ホストコンピュータ３１と端末３２は同じセッション鍵ＫＳを共有したこととなり、このセッション鍵ＫＳを用いて暗号通信を行う。具体的には、ホストコンピュータ３１の秘密情報暗号手段４９がセッション鍵ＫＳにより秘密情報ＳＩを暗号化した秘密情報データＥ（ＫＳ，ＳＩ）を生成して端末３２に送り、端末３２の秘密情報復元手段５０がこの秘密情報データＥ（ＫＳ，ＳＩ）をセッション鍵ＫＳにより復号化し、秘密情報ＳＩを復元する。そして復元された秘密情報ＳＩにより様々な処理を行うものである。

【００３２】ここで、このシステムの安全性について説明する。従来例の場合と同様に、端末３２とＩＣカード３３間は安全であるが、ホストコンピュータ３１と端末３２間は非安全であることを前提としている。ホストコンピュータ３１と端末３２間で伝送されるマスタ鍵ＮデータＥ（ＫＡ，ＫＢ）、セッション鍵データＥ（ＫＢ，ＫＳ）、秘密情報データＥ（ＫＳ，ＳＩ）を不正者が全て盗聴し、さらにＩＣカード３３を盗んだとする。この不正者がＩＣカード３３の暗証番号を知った場合、盗聴したデータをＩＣカード３３に入力し、何らかの出力をＩＣカード３３から得ることができるが、ＩＣカード３３に格納されているマスタ鍵はもはや以前のマスタ鍵Ｍ・ＫＡではなく、マスタ鍵Ｎ・ＫＢに更新されているため、不正者が欲するセッション鍵ＫＳあるいは秘密情報ＳＩを得ることはできない。すなわち、盗聴したデータＥ（ＫＡ，ＫＢ）をマスタ鍵復元手段４５に入力しても、ＩＣカードマスタ鍵格納部４２に格納されている鍵は、既にマスタ鍵Ｍ・ＫＡではなくマスタ鍵Ｎ・ＫＢであるため、何ら意味のあるデータを復元することはできない。

【００３３】ただし、もしマスタ鍵復元手段４５とセッション鍵復元手段４８および秘密情報復元手段５０が同じアルゴリズムを用いて復号化する場合、次のような手段で秘密データの取得が可能となる。すなわち盗聴したセッション鍵データＥ（ＫＢ，ＫＳ）をマスタ鍵復元手段４５に入力すると、ＩＣカードマスタ鍵格納部４２に格納されている鍵はマスタ鍵Ｎ・ＫＢであるため、マスタ鍵復元手段４５はセッション鍵ＫＳを出力する。ここで、盗聴した秘密情報データＥ（ＫＳ，ＳＩ）をセッション鍵復元手段４８に入力すれば、セッション鍵復元手段４８はＳＩを出力してしまう。

【００３４】これを防止するためには、単にマスタ鍵復元手段４５とセッション鍵復元手段４８とに異なるアルゴリズムを採用することである。そうすれば、盗聴したセッション鍵データＥ（ＫＢ，ＫＳ）をマスタ鍵復元手段４５に入力しても、本来セッション鍵Ｅ（ＫＢ，ＫＳ）はセッション鍵復元手段４８により復号化されるべきデータであるため、何ら意味のあるデータを復元することはできない。同様に、セッション鍵復元手段４８と秘密情報復元手段５０とに異なるアルゴリズムを採用する方法によっても解決できる。

【００３５】なお上記各実施の形態においては、暗号・復元化手段や更新手段および格納部を別々の構成としているが、複数の手段をまとめた構成としても同等の効果が得られることは言うまでもない。

【００３６】

【発明の効果】以上のように本発明によれば、マスタ鍵によりセッション鍵を暗号化して配送する毎に、マスタ鍵Ｍをマスタ鍵Ｎに更新することで、セッション鍵およびそれによって暗号化された秘密情報の不正な解読を防ぐことが可能となるＩＣカードおよびそれを用いた暗号通信システムを提供できる。

【図面の簡単な説明】

【図１】本発明の実施の形態１の暗号通信システムの構成図

【図２】本発明の実施の形態２の暗号通信システムの構成図

【図３】従来の暗号通信システムの構成図

【符号の説明】

１、３１　ホストコンピュータ
２、３２　端末
３、３３　ＩＣカード
１１、４１　ホストマスタ鍵格納部
１２、４２　ＩＣカードマスタ鍵格納部
１３、４７　セッション鍵暗号手段
１４、４９　秘密情報暗号手段

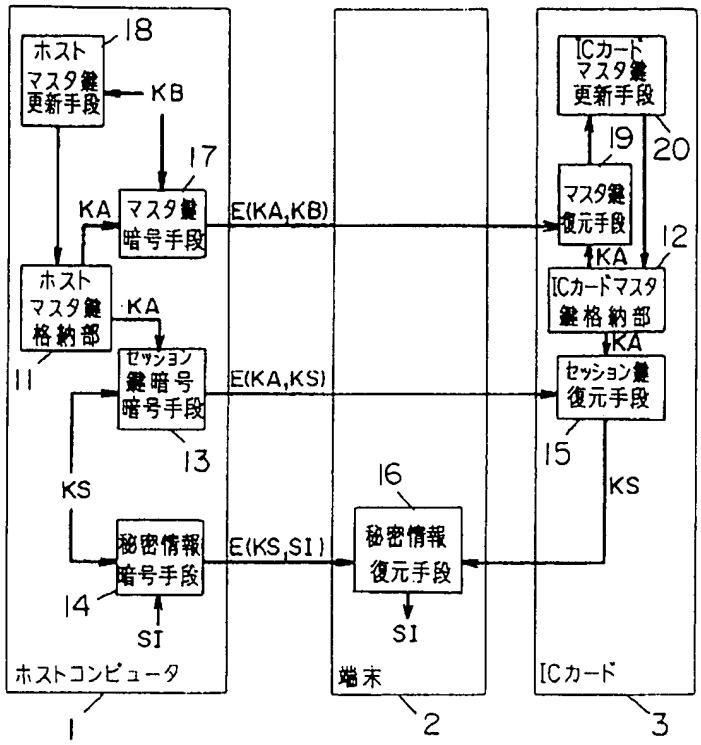
9

１５、４８　セッション鍵復元手段
１６、５０　秘密情報復元手段
１７、４３　マスタ鍵暗号手段

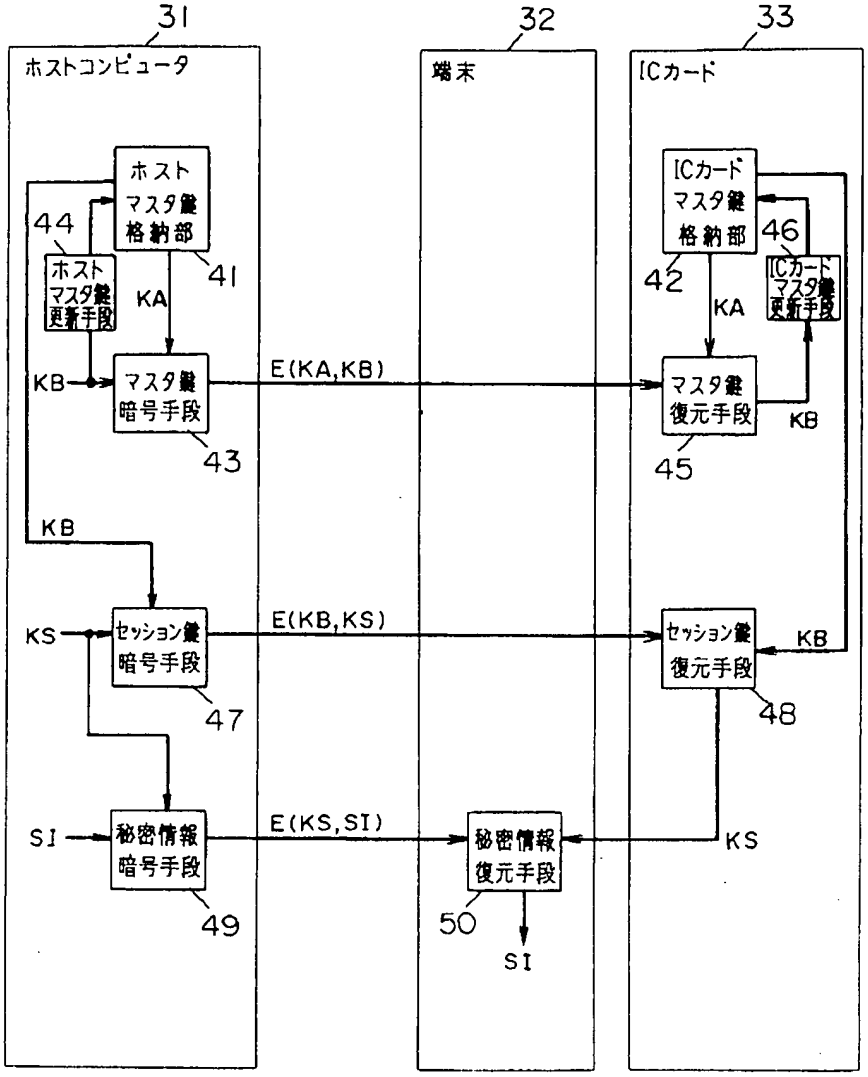
10

１８、４４　ホストマスタ鍵更新手段
１９、４５　マスタ鍵復元手段
２０、４６　ＩＣカードマスタ鍵更新手段

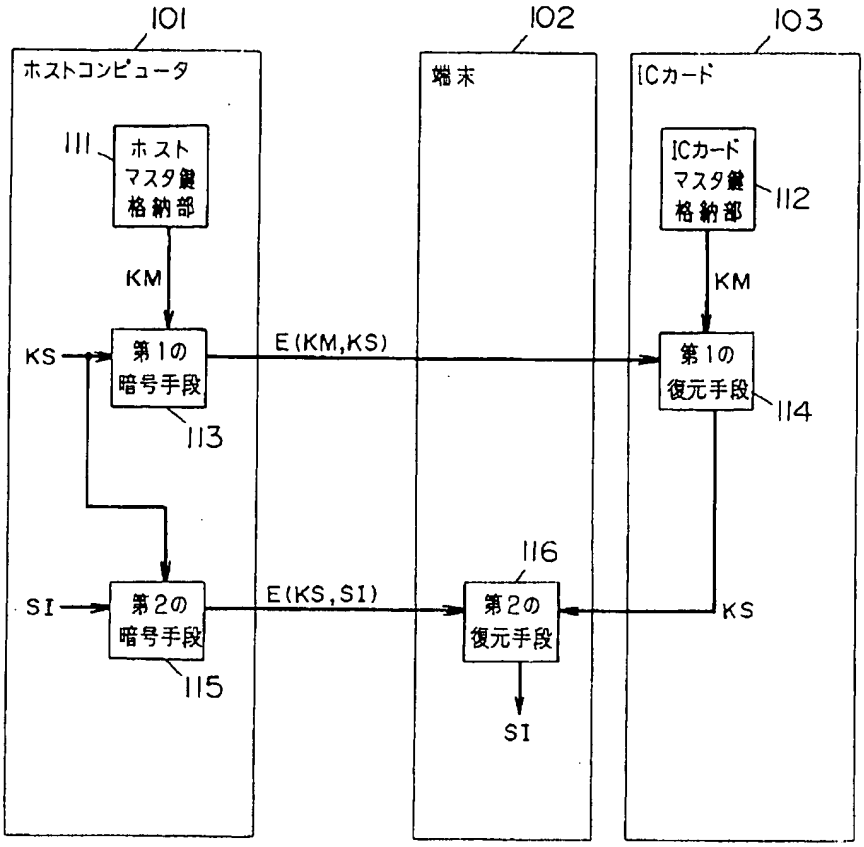
【図１】



【図２】


31
32
33
ホストコンピュータ
端末
ICカード
ホスト
マスタ鍵
格納部
41
44
ホスト
マスタ鍵
更新手段
KA
KB
マスタ鍵
暗号手段
43
E(KA,KB)
ICカード
マスタ鍵
格納部
42
46
ICカード
マスタ鍵
更新手段
KA
マスタ鍵
復元手段
45
KB
KB
KS
セッション鍵
暗号手段
47
E(KB,KS)
セッション鍵
復元手段
48
KB
SI
秘密情報
暗号手段
49
E(KS,SI)
秘密情報
復元手段
50
SI
KS

【図３】



フロントページの続き

(51) Int. Cl.[6]	識別記号	F I
		H04L 9/00　621A